# OpenSecurity Installationshandbuch zu Version 1.0

Oliver Maurhart
AIT Austrian Institute of Technology

November 25, 2014

## 1 Voraussetzungen

Das Referenzsystem zu OpenSecurity ist eine **Windows 7 SP1 64 Bit** Installation. Andere Architekturen und Betriebssystemversionen sind möglich aber nicht getestet.

Die OpenSecurity Software benutzt zur Zeit **VirtualBox 4.3.12** als Virtualisierung. VirtualBox ist von https://www.virtualbox.org/wiki/Downloads[1] frei verfügbar. Zusätzlich zur Basisinstallation benötigt OpenSecurity auch das **Oracle VM VirtualBox Extension Pack**.

## 2 Download

Die OpenSecurity Software ist als eine einzige Setup Exe Datei von http://download.opensecurity.at/downloadbar. Wir empfehlen die aktuell letzte Version von diesem Medium zu beziehen.

## 3 Installation

Die Installation erfolgt durch das Ausführen dieser Datei. Es werden dabei 3 Modi unterschieden:

1. Normal. Der User wird anhand eines Installationswizard durch die verschieden Schritte und Optionen geführt.
2. Silent. Durch Angabe von `/SILENT` als Kommandozeilenoption der Setupdatei sind keine Einstellungsmöglichgkeiten durch den Anwender auswählbar. Ein Fortschrittsbalken informiert über den Installationsvorgang. Zur Anwendung kommen hierbei die Defaulteinstellungen der Installation.
3. Very Silent. Die Angabe von `/VERYSILENT` wirkt sich wie `/SILENT` aus, jedoch wird hier auch der Fortschrittsbalken unterbunden. Es existiert kein visuelles Feedback zur Installation.

Nach einem Reboot ist OpenSecurity verfügbar.

[1] Auf einzelne Versionen von Virtualbox kann man über http://download.virtualbox.org/virtualbox/ zugreifen.

Werden nun Applikationen von OpenSecurity ausgeführt, so kann eine installierte und aktive Windows Firewall den Zugriff von

- python27
- X11-Server

vom User erstmalig über eine UAC[2] bestätigen lassen. Im Zuge der OpenSecurity 1.0 Installation werden jedoch bereits Firewall Regeln in das System eingespielt, welche diese Einstellungen vorwegnehmen.

### 3.1 Installationsdetails

Im Zuge der interaktiven Installation wird kann der OpenSecurity Standardbrowser sowie die Adresse eines Logservers angegeben werden.

- **VM Browser:** Hier wird der Pfad in der VM zur aufführbaren Datei des in OpenSecurity verwendeten Browsers angegeben. Es kann hier eine komplette Pfadangabe inklusive Parameter eingegeben werden. Der Standardwert ist "/usr/bin/chromium", welcher auf die freie Implementation des Google Chrome Browsers zeigt.
- **URL of Logserver:** Diese Eingabezeile erwartet die URL eines Logservers. Ein Logserver dient dazu, OpenSecurity relevante Ereignisse zu protokollieren. Die URL lautet in der Grundeinstellung "http://placeholder.mydomain.local:10000/logpath" – was eine ungültige, nicht existierende Adresse darstellt. Sollte im Unternehmen oder Bereich, in welchem OpenSecurity zur Ausführung kommt, ein Interesse an diesem Feature bestehen, so muss ein entsprechender Logserver installiert sein und dessen URL hier angegeben werden.

Beide Datenfelder lassen sich auch im Nachhinein von einem System Administrator in der Registry ändern.

Um auf OpenSecurity auf den aktuellsten Stand zu bringen empfehlen wir den Update-Button in den Konfigurationseinstellungen des OpenSecurity TrayIcons zu aktivieren.

## 4 Systemdetails

OpenSecurity installiert sich in `C:\Program Files\OpenSecurity`. In diesem Verzeichnis befindet sich auch das `log` Verzeichnis, in welchem OpenSecurity seine Aktionen protokolliert. Als Systemdienst legt OpenSecurity die Virtuelle Maschinen im Pfad `C:\Windows\System32\config\systemprofile` ab.

OpenSecurity installiert neben den Client (OpenSecurity TrayIcon) auch den **OpenSecurity Dienst**, welche über die Windows Dienste gestartet und gestoppt werden kann.

### 4.1 Registry

Diese Registryeinträge sind für OpenSecurity essentiell:

[2] User Account Control

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\USBSTOR`

  Hier ist der Wert der Variable **“Start”** auf **4** gesetzt. Durch neue unbekannte Medien, welche via USB eingesteckt werden, kann Windows selbst diesen Wert wieder auf **3** umstellen. Dies verhindert jedoch die Weiterreichung der USB Events an das OpenSecurity Hintergrundsystem. Es wird empfohlen via eine domainweiten Policy diesen Wert auf **4** zu fixieren.

- `HKEY_LOCAL_MACHINE\SOFTWARE\OpenSecurity`

  Unter diesem Registrypfad speichert OpenSecurity seine systemweiten Einstellungen. Zur Zeit ist die Adresse des Log Servers (**“LogServerUrl”**), welche das Speichern von Dateien auf verschlüsselte Medien protokolliert, sowie die Einstellung des zu verwendeten Browsers (**“Browser”**).

# 5 Uninstall

Um OpenSecurity zu entfernen, starten Sie wie bei anderen Installationen üblich die Systemsteuerung unter dem Punkt “Programme und Funktionen” und wählen OpenSecurity zum Entfernen an.